

1 4. On information and belief, Defendant is a Delaware corporation with its
2 principal office located at 5 Third Street, Suite 324, San Francisco, CA 94103. On
3 information and belief, Defendant may be served through its registered agent, Evan
4 Fitzgerald, at the same address, or The Corporation Trust Company, Corporation
5 Trust Center, 1209 Orange St, Wilmington, DE 19801.

6 5. On information and belief, this Court has personal jurisdiction over
7 Defendant because Defendant has committed, and continues to commit, acts of
8 infringement in this District, has conducted business in this District, and/or has
9 engaged in continuous and systematic activities in this District.

10 6. On information and belief, Defendant's instrumentalities that are alleged
11 herein to infringe were and continue to be used, imported, offered for sale, and/or sold
12 in this District.

13 **VENUE**

14 7. On information and belief, venue is proper in this District under 28
15 U.S.C. § 1400(b) because Defendant is a resident of this District. Alternatively, acts
16 of infringement are occurring in this District and Defendant has a regular and
17 established place of business in this District.

18 **COUNT I**

19 **(INFRINGEMENT OF UNITED STATES PATENT NO. 9,054,860)**

20 8. Plaintiff incorporates paragraphs 1 through 7 herein by reference.

21 9. This cause of action arises under the patent laws of the United States
22 and, in particular, under 35 U.S.C. §§ 271, *et seq.*

23 10. Plaintiff is the owner by assignment of the '860 Patent with sole rights
24 to enforce the '860 Patent and sue infringers.

25 11. A copy of the '860 Patent, titled "Digital Verified Identification System
26 and Method," is attached hereto as Exhibit A.

27 12. The '860 Patent is valid, enforceable, and was duly issued in full
28 compliance with Title 35 of the United States Code.

1 13. Upon information and belief, Defendant has infringed and continues to
2 infringe one or more claims, including at least Claim 1, of the ‘860 Patent by making,
3 using (at least by having its employees, or someone under Defendant's control, test
4 the accused Product), importing, selling, and/or offering for sale associated hardware
5 and/or software for digital communication services (e.g., Paubox Email Suite
6 service), and any similar products and/or services (“Product”) covered by at least
7 Claim 1 of the ‘860 Patent. Defendant has infringed and continues to infringe the ‘860
8 patent either directly or through acts of contributory infringement or inducement in
9 violation of 35 U.S.C. § 271.

10 14. The Product provides a system for e-signatures. The Product provides
11 for digitally verifying the identification of a sender. Certain aspects of this element
12 are illustrated in the screenshot(s) below and/or in those provided in connection with
13 other allegations herein.

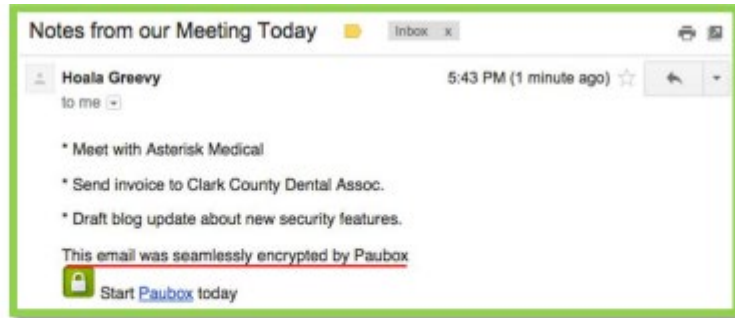
Paubox Email Suite: How does it work?

A simple way to think about the process is Paubox acts as a concierge for your email. Our encryption service sits on your email server and touches each email as you send it. The result?

ALL of your outbound email goes through our email encryption service, which enforces 256-bit AES encryption on all of your email, from every device, and every user.

What could be better than that? That little Paubox concierge sitting on your server will also guarantee **EVERY EMAIL IS DELIVERED ENCRYPTED!**

Source: <https://www.paubox.com/blog/paubox-encrypted-email/>



Source: <https://www.paubox.com/blog/paubox-encrypted-email/>

15. The Product includes at least one digital identification module structured to be associated with at least one entity. For example, the Product provides a module (e.g., private keys for a user) to be associated with at least one entity (i.e., a user who needs to send an encrypted email). Certain aspects of this element are illustrated in the screenshot(s) below and/or in those provided in connection with other allegations herein.

Paubox also supports DKIM, which authenticates emails through a pair of public and private cryptographic keys. DKIM discourages spammers from spoofing email domains and protects recipients from email phishing attacks.

Source: <https://www.paubox.com/blog/top-7-things-didnt-know-paubox-email-suite/>

What is DKIM and how does it work?

By definition, DomainKeys Identified Mail (DKIM) is a method that authenticates emails through a pair of cryptographic keys - a public key published in a Domain Name System TXT record and a private key encrypted in a signature affixed to outgoing messages. Both keys are generated by the domain owner.

Source: <https://www.paubox.com/blog/what-is-dkim-and-why-you-need-it/>

Paubox offers a comprehensive set of features and services to make key management and encryption of PHI easy to manage and simpler to audit, including the Key Management Service (KMS). Master keys in KMS can be used to encrypt/decrypt data encryption keys used to encrypt customer PHI. Data encryption keys are protected by customer master keys stored in KMS, creating a highly auditable key hierarchy as API calls to KMS are logged.

Source: <https://www.paubox.com/content/security/>

What are the requirements of S/MIME?

S/MIME is based on public key cryptography. This form of encryption is widely understood by computer scientists, but is difficult to explain to the average person. Key components include certificate authorities, certificates, public and private keys, key escrow and exchange systems and signatures.

For example, while Google's commercial email service supports S/MIME, using it requires a third-party security certificate for the organization, as well as a certificate for each individual email address. And to establish a secure email connection, both sender and receiver will need to exchange encryption keys. If either party doesn't have S/MIME configured or doesn't have the other party's key, S/MIME will not work, and the email will not be delivered.

Source: <https://www.paubox.com/blog/what-is-s-mime/>

16. The Product includes a module generating assembly (sign up page) structured to receive at least one verification data element corresponding to the at least one entity (e.g., a user has to sign up using a unique login ID and password for encrypting the emails and the documents) and create said at least one digital identification module (i.e., creation/generation of encryption key for the user). Certain aspects of this element are illustrated in the screenshot(s) below and/or in those provided in connection with other allegations herein.

1 Hey There!

2 **Let's get started**

3

4 Organization Name*

5

6 Email*

7

8

9 Name*

10

11 **CONTINUE**

12

13 Paubox Email Suite

14 **Standard**

15 ✓ 14-day Free Trial

16 ✓ **Send Encrypted Email**

17 ✓ Business Associate Agreement

18 ✓ HIPAA Compliant

19 ✓ HITRUST CSF Certification

20

21

22

23

24

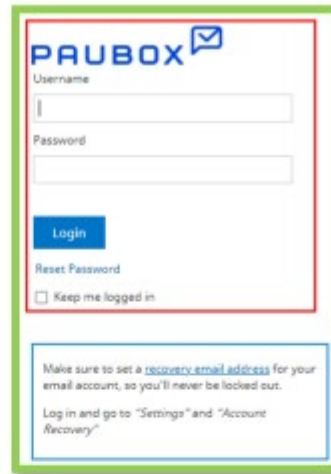
25

26

27

28

Source: https://app.paubox.com/new_wizard/new?order_name=paubox_suite_order&plan_name=standard&unit_count=1



PAUBOX

Username

Password

Login

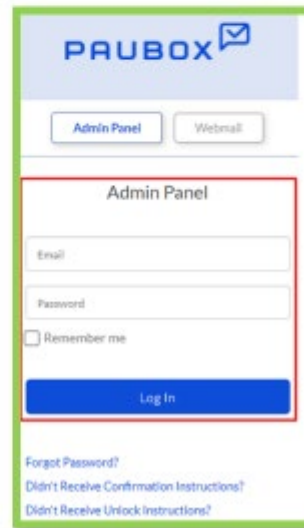
Reset Password

☐ Keep me logged in

Make sure to set a [recovery email address](#) for your email account, so you'll never be locked out.

Log in and go to "Settings" and "Account Recovery"

Source: <https://m.paubox.com/mail/>



PAUBOX

Admin Panel Webmail

Admin Panel

Email

Password

☐ Remember me

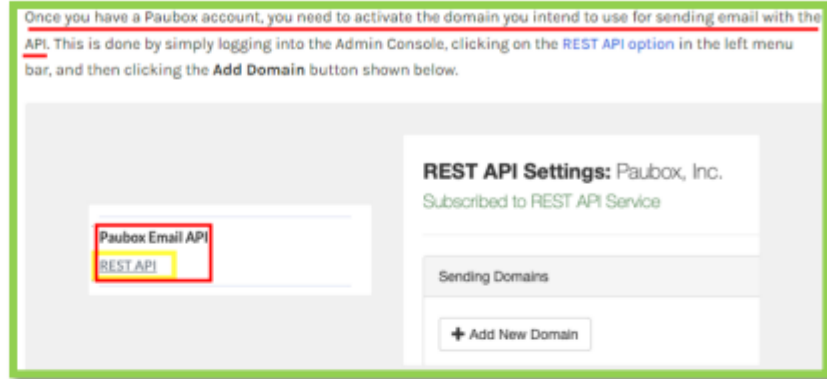
Log In

Forgot Password?

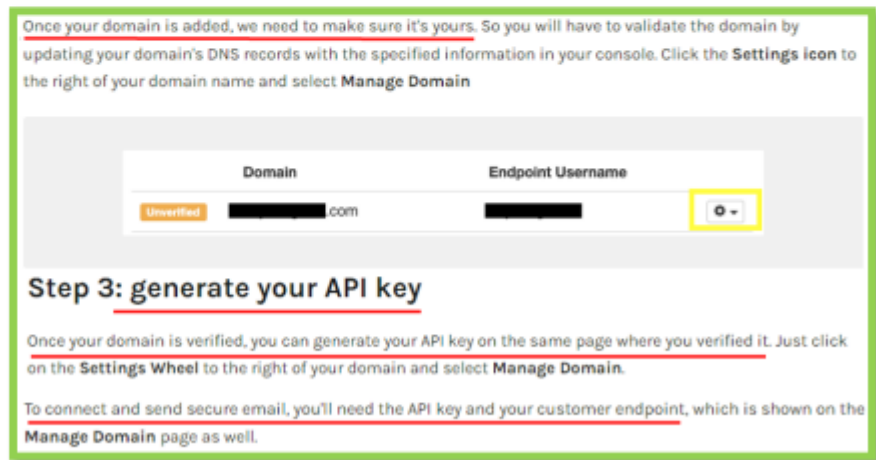
Didn't Receive Confirmation Instructions?

Didn't Receive Unlock Instructions?

Source: https://app.paubox.com/users/sign_in?demo_type=orca&m=show



Source: https://docs.paubox.com/docs/paubox_email_api/quickstart/



Source: https://docs.paubox.com/docs/paubox_email_api/quickstart/

17. The at least one digital identification module (encryption key) is disposable within at least one electronic file (content or attachments, etc.). Certain aspects of this element are illustrated in the screenshot(s) below and/or in those provided in connection with other allegations herein.

1 Are my attachments encrypted?

2
3
4 Yes, all attachments are encrypted. Paubox supports attachments up to 50MB.

5 Source: <https://www.paubox.com/content/pricing/#paubox-suite>

6 Every Paubox account comes with one encrypted email address and
7 one encrypted contact form.

8
9 You can attach encrypted contact forms to your website or send it
10 through an email.

11 The contact form link will be hosted on our secure Paubox server, so
12 you don't need to worry about [having a HIPAA compliant website](#) and
13 server.

14
15 Source: <https://www.paubox.com/blog/how-patients-send-hipaa-compliant-email-first/>

Use a secure URL to receive secure messages from patients

There is no way a patient can send you a secure email first without having email encryption in place themselves. However, a Paubox encrypted contact form is a seamless workaround for patients to send secure messages to their healthcare providers.

Our Paubox encrypted contact form features basic fields for patients to fill in, such as their name, email address, phone number, and a brief message. We'll also include a space where patients can upload up to 50 megabytes of attachments (such as photos or documents).

Patients can access the encrypted contact form through a secure, custom URL that can be placed anywhere on your website. This allows the patient to send a secure message to your organization first, and the information will be delivered in a HIPAA compliant email straight to your inbox, avoiding the hassle of hard copies, scanning and manual entry.

Source: <https://www.paubox.com/blog/how-patients-send-hipaa-compliant-email-first/>

Paubox offers a comprehensive set of features and services to make key management and encryption of PHI easy to manage and simpler to audit, including the Key Management Service (KMS). Master keys in KMS can be used to encrypt/decrypt data encryption keys used to encrypt customer PHI. Data encryption keys are protected by customer master keys stored in KMS, creating a highly auditable key hierarchy as API calls to KMS are logged.

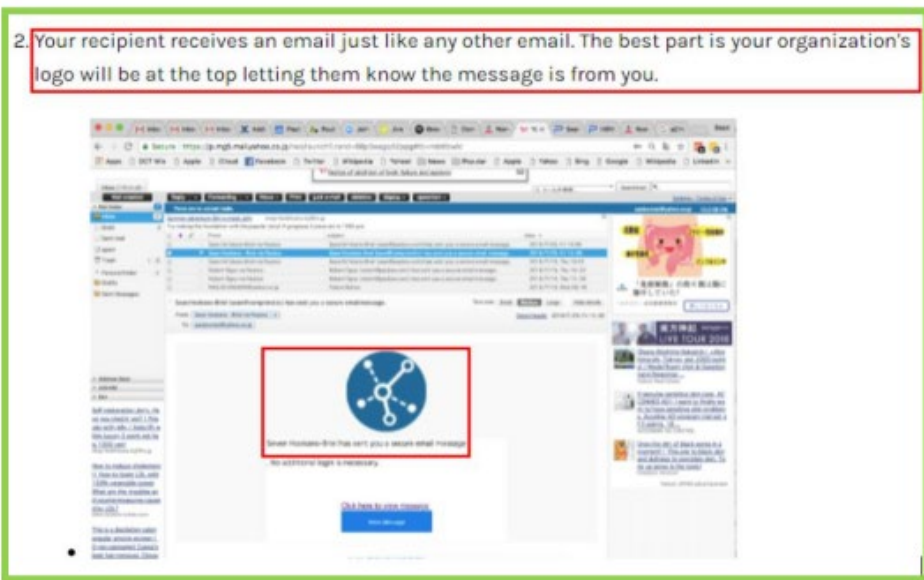
Source: <https://www.paubox.com/content/security/>

18. The at least one digital identification module includes at least one primary component structured (e.g., a metadata text indicating encrypted text) to at least partially associate said digital identification module with said at least one entity (e.g., the user, who has sent the encrypted email). Certain aspects of this element are illustrated in the screenshot(s) below and/or in those provided in connection with

other allegations herein.



Source: <https://support.paubox.com/hc/en-us/articles/360007494534-How-to-Read-and-Reply-to-a-Paubox-Secure-Message>



Source: <https://support.paubox.com/hc/en-us/articles/115003551868-Secure-Notification-emails>

To assure your recipients that the email you sent is encrypted, they will see a neat little digital signature at the footer of your email saying that your email was encrypted for their safety and security by Paubox.

Source: <https://www.paubox.com/blog/gmail-encryption-settings/>

1 19. The at least one digital identification module (i.e., user's private key) is
 2 cooperatively structured to be embedded within only a single electronic file (e.g.,
 3 encryption key is stored within a document including email, other documents attached
 4 etc.). Certain aspects of this element are illustrated in the screenshot(s) below and/or
 5 in those provided in connection with other allegations herein.

6 Paubox also supports DKIM, which authenticates emails through a
 7 pair of public and private cryptographic keys. DKIM discourages
 8 spammers from spoofing email domains and protects recipients
 9 from email phishing attacks.

10 Source: <https://www.paubox.com/blog/top-7-things-didnt-know-paubox-email-suite/>

11 Every Paubox account comes with one encrypted email address and
 12 one encrypted contact form.

13 You can attach encrypted contact forms to your website or send it
 14 through an email.

15 The contact form link will be hosted on our secure Paubox server, so
 16 you don't need to worry about having a HIPAA compliant website and
 17 server.
 18

19 Source: <https://www.paubox.com/blog/how-patients-send-hipaa-compliant-email-first/>

20 Paubox offers a comprehensive set of features and services to make key management and encryption of
 21 PHI easy to manage and simpler to audit, including the Key Management Service (KMS). Master keys in
 22 KMS can be used to encrypt/decrypt data encryption keys used to encrypt customer PHI. Data encryption
 23 keys are protected by customer master keys stored in KMS, creating a highly auditable key hierarchy as API
 24 calls to KMS are logged.

25 Source: <https://www.paubox.com/content/security/>

20. Defendant's actions complained of herein will continue unless Defendant is enjoined by this court.

21. Defendant's actions complained of herein are causing irreparable harm and monetary damage to Plaintiff and will continue to do so unless and until Defendant is enjoined and restrained by this Court.

22. Plaintiff is in compliance with 35 U.S.C. § 287.

JURY DEMAND

23. Under Rule 38(b) of the Federal Rules of Civil Procedure, Plaintiff respectfully requests a trial by jury on all issues so triable.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff asks the Court to:

(a) Enter judgment for Plaintiff on this Complaint on all causes of action asserted herein;

(b) Enter an Order enjoining Defendant, its agents, officers, servants, employees, attorneys, and all persons in active concert or participation with Defendant who receive notice of the order from further infringement of United States Patent No. 9,054,860 (or, in the alternative, awarding Plaintiff a running royalty from the time of judgment going forward);

(c) Award Plaintiff damages resulting from Defendant's infringement in accordance with 35 U.S.C. § 284;

(d) Award Plaintiff pre-judgment and post-judgment interest and costs; and

(e) Award Plaintiff such further relief to which the Court finds Plaintiff entitled under law or equity.

Dated: November 2, 2021

Respectfully submitted,

/s/ Stephen M. Lobbin

Attorney(s) for Plaintiff